Vulnerability Assessment Report

Completed by Wren Wilson on April 7th, 2025

System Description

As provided:
“The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.”

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database is central to the functionality of the business. It includes data from relevant stakeholders, such as employees and customers, as well as historical files and future projects. Securing its data is key for preventing interference and protecting company functionality from being negatively impacted by both inside and outside threats. Without the server, the business would not be able to operate as intended, potentially damaging its reputation and bottom line.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	Disrupt mission-critical operations	2	3	6
Customer	Alter/Delete critical information	1	2	2
System administration	Obfuscate future attacks	2	3	6
Competitor	Perform reconnaissance and surveillance of organization	1	2	2
Hacker	Obtain sensitive information via exfiltration	3	3	9

Approach

Risks analyzed the business's system and its current management, as well as customer and employee interactions with it. Likelihood of a threat occurrence was compared to the resulting severity the threat would have on the company's operations and classified accordingly. Human error and suspected outside malice were also taken into consideration.

Remediation Strategy

Controlling employee and customer access through least privilege, monitoring suspicious activity through intrusion detection systems, as well as internal auditing to protect against internal threat actors. Strong password requirements, two-factor authentication through push notifications as text messages and phone calls can be intercepted, and further data encryption is also recommended. All networks, even guest wi-fi, should be password protected and have ample firewall coverage.